BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan dunia jaringan telekomunikasi pada saat ini sangat cepat bersamaan dengan tingginya peningkatan akan kebutuhan layanan yang cepat dan efisien [1]. Sama halnya dengan komunikasi data, mulai dari hubungan antar dua komputer hingga sebuah jaringan komputer yang kompleks. Hal itu membuat jumlah perangkat yang terhubung ke jaringan internet semakin bertambah banyak setiap saat [2]. Dengan berkembangnya teknologi jaringan internet tentu saja akan sangat memudahkan kehidupan manusia. Namun sebaliknya, hal ini sekaligus telah menyebabkan peningkatan dalam jumlah serangan berbasis jaringan itu pula [2].

Berkaitan dengan masalah keamanan yang merupakan salah satu elemen penting dalam sebuah sistem informasi dan jaringan, dalam kenyataannya sering kali dikesampingkan oleh administrator jaringan karena dianggap kurang terlalu penting dan sering kali malah dikurangi atau bahkan dihilangkan dengan alasan mengganggu performansi dari sistem itu sendiri [3].

Dengan demikian pada akhirnya yang menjadi masalah adalah saat sebuah ancaman sudah mulai menimbulkan suatu kerugian karena terlambat untuk ditangani, dan pada saat itulah administrator jaringan akan mulai sadar betapa pentingnya suatu sistem keamanan dan sesegera mungkin akan melakukan berbagai macam tindakan perbaikan atas keamanan sistem informasi jaringan [4].

Berdasarkan penelitian yang telah dilakukan Kaspersky Labs, diperkirakan terjadi percobaan serangan terhadap jaringan komputer sekitar 580 juta kali dalam hitungan hari [2]. Melihat begitu banyaknya percobaan serangan terhadap jaringan komputer yang semakin lama semakin bervariasi dalam hal metode yang digunakan, mengaplikasikan mekanisme pertahanan

kemanan jaringan untuk mengenali berbagai jenis serangan-serangan ini adalah hal yang sangat penting [2].

Keamanan akan data-data elektronik akan sangat penting adanya baik untuk keperluan jaringan skala besar maupun kecil, karena merupakan salah satu unsur penting dalam teknologi informasi. Keamanan akan data-data elektronik secara tidak langsung dapat berpengaruh dalam kepastian proses keberlanjutan suatu bisnis atau usaha, mengurangi risiko, dan mencari kesempatan bisnis atau usaha [5].

Maka dari itu jika suatu sistem keamanan yang dibangun tidak cukup baik maka secara otomatis akan berdampak besar dalam seluruh kegiatan yang berhubungan langsung dengan dunia jaringan. Selain data-data pribadi yang rentan diretas, kondisi terhadap performa sistem juga akan terganggu akibat dari suatu sistem keamanan yang tidak cukup baik, contoh sederhananya adalah penurunan terhadap kinerja sistem. Selain itu masalah nama baik suatu perorangan atau organisasi juga akan terdampak dari suatu mekanisme keamanan jaringan yang tidak cukup baik tersebut.

Implementasi suatu mekanisme keamanan informasi jaringan yang baik didapatkan melalui seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan perangkat lunak [5]. Dari sekian banyak jenis perangkat lunak yang difungsikan khusus sebagai mekanisme keamanan jaringan, satu diantaranya adalah menggunakan *Cowrie Honeypot* [2].

Dalam sebuah penelitian yang dilakukan oleh R. M Campbell, K. Padayachee dan T. Masombuka , pada sebuah jurnal yang berjudul *"A Survey of Honeypot Research: Trends and Opportunities"* menyatakan bahwa *Honeypot* dapat digunakan untuk menangkap penyusup jaringan dan juga mempelajari teknik yang digunakan oleh penyusup ini untuk mendapatkan akses ke sistem jaringan [2]. Penelitian tersebut melibatkan dan mempelajari berbagai sumber dan referensi tentang *Cowrie Honeypot* sebagai tingkatan baru keamanan jaringan, namun hanya sebatas survei terhadap tren yang sedang berkembang terkait dengan sistem *Cowrie Honeypot* termasuk dengan

segala fitur didalamnya, tanpa terkecuali sistem monitoring konvensional berbasis terminal yang tidak semua orang mengerti akan *output* yang ditampilkan. Akibatnya akan sulit untuk dilakukan analisis terhadap data yang masuk dari hasil monitoring.

Penyajian suatu bentuk informasi dalam komputer yang baik adalah yang dilakukan dengan prosedur penyajian program aplikasi yang di rancang secara sistematis dan baik sehingga dapat diakses dan di mengerti oleh semua pengguna [6]. Ketika pengguna berkunjung ke dalam program aplikasi tersebut, diharapkan pengguna akan terkesan dan tertarik kemudian ingin mengeksplorasi sebanyak mungkin segala bentuk informasi yang ada di program aplikasi tersebut, maka dari itu untuk menyajikan program aplikasi yang baik tidak luput dari perancangan program aplikasinya dan tidak luput pula dari desain visual dan informasi yang termuat didalamnya [6].

Berdasarkan beberapa pembahasan diatas penulis ingin merancang dan membangun serta mengimplementasikan sebuah mekanisme keamanan jaringan menggunakan *Cowrie Honeypot* dengan prioritas utama pada keamanan media interaksi *shell* SSH (Secure Shell) yang dipadukan dengan sistem monitoring berbasis web, untuk memudahkan administrator jaringan dalam pemantauan sistem secara langsung dengan tampilan yang mudah untuk dipahami, sehingga dapat diambil analisis dan langkah penanganan yang tepat terhadap situasi yang sedang terjadi pada sistem.

1.2. Rumusan Masalah

Bagaimana meningkatkan keamanan jaringan pada media interaksi *shell* SSH (Secure Shell) menggunakan *Cowrie Honeypot* yang dipadukan dengan sistem monitoring berbasis web untuk menjaga keamanan data dan informasi pribadi serta mempertahankan performa sistem agar tetap pada kondisi baik yaitu tetap *up* atau tidak mengalami *down*?

1.3. Batasan Masalah

Mengingat mekanisme yang digunakan dalam sistem keamanan jaringan menggunakan *Cowrie Honeypot* terdiri dari berbagai macam metode

dan tipe interaksi terhadap respon serangan dari luar sistem, maka dalam hal ini perlu terdapat batasan masalah yang pasti terkait metode dan tipe interaksi apa yang akan digunakan dan diselesaikan dalam penelitian ini. Adapun batasan masalah pada penelitian ini sebagai berikut:

Tipe interakasi *Honeypot* yang diterapkan adalah tipe interaksi sedang, dimana sistem *Honeypot* berfungsi sebagai emulator dari beberapa layanan dari sistem operasi, namun masih belum memiliki sistem operasi yang nyata [7].

1.4. Tujuan Penelitian

Membuat sistem monitoring keamanan jaringan pada media interaksi *shell* untuk memonitor keamanan data dan informasi pribadi serta mempertahankan performa sistem agar tetap pada kondisi baik yaitu tetap *up* atau tidak mengalami *down*.

1.5. Manfaat Penelitian

a. Mempermudah pekerjaan manusia untuk aktifitas analisis data.
b. Mempercepat proses analisis data dari data mentah menjadi data yang sudah siap disajikan.
c. Mempercepat proses pemrosesan data dalam skala yang besar.